Guidelines for a Seamless Wireless Network Upgrade

Prepared by
Loendry Antonio Madueno Leal

CONTENTS

Melissa Rowland | Global Account Executive (Sales) melissa@cwnp.com cwnp.com

LIST OF FIGURES

INTRODUCTION

As users become increasingly mobile and business applications require a more interactive approach, the strategic importance of innovative wireless services in helping companies maintain innovation, agility, and differentiation becomes clear. By migrating to a next-generation wireless network, the correct platform can deliver the performance and reliability needed to support multimedia and business-critical applications wherever mobile connectivity is required. This upgrade is not just a technical move but a strategic one that can significantly impact a company's competitiveness and, more importantly, the user experience.

The evolution of the Wi-Fi world over the last five years, where users rely increasingly on wireless networks to perform their daily jobs while maintaining elevated levels of security and privacy, underscores the strategic importance of this upgrade. A wireless migration to upgrade an existing network and provide more reliability to the end user is a monumental task, including multiple teams, an elevated level of coordination and effort, plus a long-term cycle that can last, in many cases, various years depending on the size of the network. During this time, architects, project managers, engineers, and contractors will be engaged daily to achieve the final goal, including replacing existing wireless controllers, switches, routers, and access points. Each component is critical for the wireless network to function as needed. The ultimate goal of this upgrade is to enhance the user experience significantly.

I will explore a scenario I have managed multiple times in the last six years. This process will include some best practices and considerations for performing a wireless migration/upgrade in an enterprise-level environment without affecting the end users. All considerations will be exercised using Cisco wireless controllers, switches, routers, and access points as a reference.

SCOPE OF WORK

This case study contemplates a wireless network, mostly 802.11n and 802.11ac devices installed across multiple buildings (Cisco 3700 and 3800 APs). The company requesting the upgrade has around 2500 APs, each appropriately configured depending on the business application needed per location. To accomplish the task, new controllers and APs were purchased for the layer 2 infrastructure, network switches installed are 9300 series capable of UPoE and layer 3 routers are Cisco 9500 series. I staged, configured, and deployed two 9800 Cisco WLCs and 2500 APs (9120axe and 9120axi).

Figure 1. Cisco 9800 Wireless Controller

DEFINITION AND DESIGN

The architecture team defined the project as a complete upgrade/migration starting with the staging, configuring, and deploying the two wireless controllers, Cisco C9800-80-K9. I created all the WLANs, RF profiles and site tags based on the stakeholders' needs. Each Business Unit leadership team was interviewed and asked basic questions regarding expectations, coverage, mobility, and commonly used applications. Based on this feedback, two main SSIDs were needed to support the business: WLAN-Corp and Internet-Corp. The first SSID provides access to all internal applications related to employees, network access, change control, monitoring, etc. The second SSID is an Internet access WLAN for guests, contractors, and vendors. Each location has a site tag to identify the building, the number of APs supported, plus a 10% buffer for future growth. For example, "Building 100" has around 320 APs, and the site tag will help 350 APs. Regarding RF Tags/Profiles, there will be two: Corp-Indoor and Corp-Outdoor.

PROOF OF CONCEPT

Controllers

I staged and tested the equipment beforehand to make a seamless transition to the new network; the process starts with the wireless controllers. A pair of Cisco 9800s were used in this case. A lab environment is necessary to begin the process, so the equipment is isolated from the production network. 9800 controllers were racked, and 4 uplinks were used for each. Single-mode fiber using 10G SFP+ Cisco transceivers connect them to the routers, forming a port channel capable of 40 Gbps. Controllers were inter-connected utilizing an ethernet cable on their redundancy port. They can establish a layer 2 connection using a designated VLAN to move the traffic and pair up on stateful switchover mode (SSO).

Additionally, these controllers can communicate using a Layer 3 Redundancy Manager Interface or RMI, which is a point-to-point connection. After a successful pre-configuration and pairing, the controllers are ready to be fully configured. Once they are, they will move to the production network in preparation for the first phase of AP migration. Below are four key features that make these wireless controllers the right choice for this enterprise environment:

Wireless	IEEE 802.11a, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11n, 802.11k, 802.11r, 802.11u, 802.11w, 802.11ac Wave 1 and Wave 2, 802.11ax
Wired, switching, and routing	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX, 1000BASE-T, 1000BASE-SX, 1000-BASE-LH, IEEE 802.1Q VLAN tagging, IEEE 802.1AX Link Aggregation
Encryption standards	▪ Static Wired Equivalent Privacy (WEP) RC4 40, 104 and 128 bits ▪ Advanced Encryption Standard (AES): Cipher Block Chaining (CBC), Counter with CBC-MAC (CCM), Counter with CBC Message Authentication Code Protocol (CCMP) ▪ Data Encryption Standard (DES): DES-CBC, 3DES ▪ Secure Sockets Layer (SSL) and Transport Layer Security (TLS): RC4 128-bit and RSA 1024- and 2048-bit ▪ DTLS: AES-CBC ▪ IPsec: DES-CBC, 3DES, AES-CBC ▪ 802.1AE MACsec encryption
Management interfaces	▪ Web-based: HTTP/HTTPS ▪ Command-line interface: Telnet, Secure Shell (SSH) Protocol, serial port ▪ SNMP ▪ NETCONF

Figure 2. 9120 access point features

WLANS

In this stage, the controllers are up and running the Cisco recommended IOS, SMU (Software Maintenance Upgrade), and AP services packs (ASPS). Creating the WLANs, RF Profiles, and Site Tags starts from here. Based on the expectations from the Business Units, I created the corporate SSID with 802.1x security, which will leverage a ClearPass Aruba Server as the authentication server running RADIUS. Other considerations include Fast Transition (FT), MU-MIMO (Uplink and downlink), and 802.11k. Secondly, I created the Internet-Corp SSID to use a captive portal to register the user's device's mac address, name, last name, and email address.

RF Profiles

In preparation for the proof of concept, two main RF profiles were created, 1 for indoor and 1 for outdoor applications. Each profile was split up based on the RF band, so each has a 2.4 GHz, 5 GHz, and 6 GHz variant. The focus here remains on the two upper bands, as the whole point of the network upgrade is to emphasize the use of the 5 GHz and 6 GHz features and capabilities provided by the new controllers and APs. Regarding the basic RF setup, all legacy data rates were disabled, making 24 Mbps mandatory, channel bonding is active using 40 MHz channels, and the maximum allowed clients per AP is set to 100 users. Cisco controllers use dynamic channel assignments (DCA) based on a feature called RRM (Radio resource management); every 10 minutes, the WLC runs a scan on the network using the APs online and determines the best channel and power settings necessary to satisfy the client load per AP and avoid co-channel interference and drops, this setup will be validated once there is more traffic on the network, and adjustments will be made if necessary.

Site Tags

Each building has its site tag that identifies the location and includes the maximum number of APs supported. Cisco 9800 controllers used the site tags and the load factor (number of APs) to determine the internal memory resources needed to manage the workload for the APs on a specific site. The WLC classifies the location and relates it to a WNCD process. Each WCND process internally will manage all users' traffic on the APs. A load balance approach is mandatory to use the WLC resources appropriately. Having processes with more load than expected will cause clients to drop and issues during roaming.

ACCESS POINTS

The local team evaluated each building using the Ekahau site survey software to determine the number of APs needed for the upgrade. By performing this predictive site survey per building and floor, the design team ensures that the network coverage will be accurate and that the correct AP is installed in critical areas of high traffic, like conference rooms and lobbies. For this case, 1 AP model was chosen, specifically the Cisco 9120 AXI/AXE. These APs provide the IEEE 802.11ax Wi-Fi 6, which delivers a better experience in typical environments with more predictable performance for advanced applications such as 4K or 8K video, high-density, high-definition collaboration apps, all-wireless offices, and IoT. These APs can also have multi-gigabit connectivity: 100 Mbps, 1 Gbps and 2.5 Gbps.
I staged all APs in the lab, where 3 switches were installed for multiple APs to come online in one shot and be provisioned by batches. Another point to keep in mind is the AP naming convention. A primary spreadsheet must constantly be updated and accurate to keep track of the APs configured. APs were named based on the building number and location. The name format is bxxx-location-ap, for instance, b100 Lobby AP-> b100-lobby-01-ap.

Figure 3. Cisco 9120axi access point

802.11ax	▪ 4x4 downlink MU-MIMO with four spatial streams ▪ Uplink/downlink OFDMA ▪ TWT ▪ BSS coloring ▪ MRC ▪ 802.11ax beamforming ▪ 20-, 40-, 80-, and 160-MHz channels ▪ PHY data rates up to 5.38 Gbps (160 MHz with 5 GHz and 20 MHz with 2.4 GHz) ▪ Packet aggregation: A-MPDU (transmit and receive), A-MSDU (transmit and receive) ▪ 802.11 DFS ▪ CSD support

Figure 4. 9120 access point 802.11ax capabilities

DHCP Server

As part of the process of staging and configuring APs, it's necessary to have the appropriate VLAN setup on all switch ports; keep in mind this VLAN will allow the APs to obtain a management IP address, making them visible on the network from a layer 3 perspective. For this case, I am considering Infoblox as the DHCP server in use, with multiple VLANs serving as management VLANs. The range used for this example is VLAN 700 to 705, each capable of managing 500 APs, as the rest of the IPs are reserved as gateway SVIs and for other management purposes.

VLAN 701: 10.68.128.0/23, usable range -> 10.68.128.1 - 10.68.129.254 -> Buildings 100 & 200
VLAN 702: 10.68.130.0/23, usable range -> 10.68.130.1 - 10.68.131.254 -> Buildings 300 & 400
VLAN 703: 10.68.132.0/23, usable range -> 10.68.132.1 - 10.68.133.254 -> Buildings 500 & 600
VLAN 704: 10.68.134.0/23, usable range -> 10.68.134.1 - 10.68.135.254 -> Buildings 700 & 800
VLAN 705: 10.68.136.0/23, usable range -> 10.68.136.1 - 10.68.137.254 -> Buildings 900 & 1000

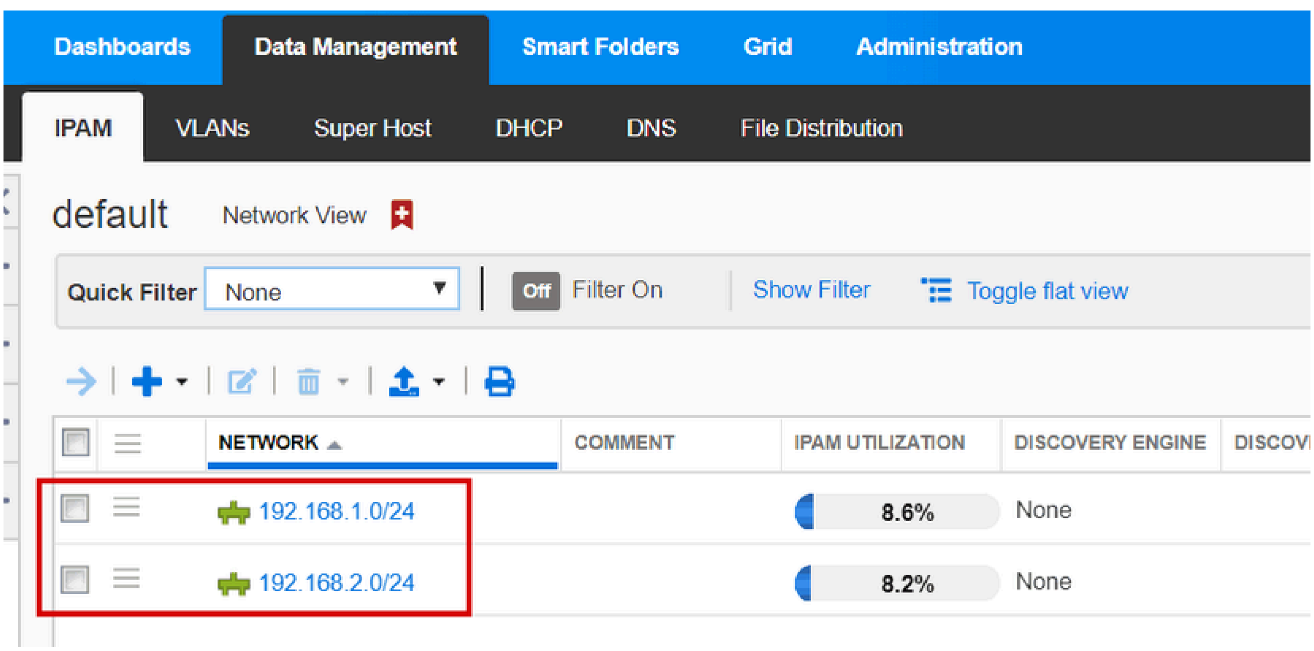

Figure 5. Infoblox Graphic User Interface

Melissa Rowland | Global Account Executive (Sales)   melissa@cwnp.com   cwnp.com

Soft-Migration – Proof of concept validation

Before going into a large-scale wireless network upgrade and executing a large AP migration on a corporate environment, performing a soft migration is recommended to validate that the steps taken into consideration during the proof of concept are working. Based on the feedback from the business units, the parking lot for building 100 was selected as the designated location for the evaluation. This area has 50 APs, Cisco model 3702 external. So, to assess the wireless controller configuration as well as the basic parameters like RSSI, SNR and throughput, the following steps were executed:

1. Verify # of APs to migrate.
2. Check the wireless controllers to ensure all necessary WLANs, RF tags, and sites are created.
3. Create a method of procedure (MOP) and a change record using the designated change control management tool (Service Now).
4. Request a change review and approval from the vendor (Cisco), the business unit involved from building 100, the team leader and manager for your department, and finally, corporate CAB.
5. Once the change is approved, it will be implemented during a previously established maintenance window. This window must be designed not to affect any clients who work in the facilities, even if it is a third-shift situation where workers are just performing maintenance.
6. Migrate the APs from the old controller (Cisco 5500 or 8500 series) by changing the primary controller's name and IP address and rebooting the APs.
7. Once the APs join the new controller, as a 1st step, they will upgrade their code.
8. APs now entirely online will require new configuration, which will be the WLANs, RF, and site tags created during the initial phase of the controller setup.

9. Once the APs are configured and operational, the last portion, which involves validation, will start.
10. To validate that the configuration is accurate, an on-site tech/engineer providing remote support will be at the designated area to connect to both WLAN-Corp and the Internet-Corp SSIDs.
11. SNR, RSSI and roaming were evaluated for each network as part of the process.
12. Once validation is completed, plan the next wave of APs to be moved and close the change record as successful.

By performing these steps, I tested all the new wireless network infrastructure, specifically layers 1 and 2, the domain under the new wireless controller. The idea is to repeat this process as often as necessary to move all the existing APs to the new wireless controllers. This process can take a long time since each location must be evaluated and requires the business unit to agree each time. This will guarantee the new APs will be deployed with minimum downtime.

Implementation

In this phase, the network is ready for a complete upgrade as the core equipment is in place, tested and working as expected. As mentioned above, this phase requires a lot of coordination between multiple groups, specifically engineering and the contractor-3rd party installing the APs. From this point, it will be assumed that all the old APs (3700s and 3800s) have been moved to the new controllers. We are moving towards the Wi-Fi 6 upgrade by installing the new 9120axi/axe access points. Engineering will keep provisioning new APs per the architecture design spreadsheet and documenting all names, serial numbers, models, and Mac addresses so asset management is implemented correctly. Installing the devices will require overnight shifts and small areas of impact on the business. The 3rd party contractor, in conjunction with the project manager and engineering team, should devise a schedule flexible enough to avoid downtime in critical areas.

Usually, around 25 to 30 access points are installed per night between 2 am and 6 am local time, as this is the usual maintenance window and when network traffic is minimal. Weekly calls with all parties involved are mandatory; on a project of this scale, the project manager's role is to keep track of the progress made daily by all teams and address any concerns that can arise at a specific location or might need immediate attention.

Besides the effort from engineering and the contractor, there are two other components to consider. First, we have monitoring tools alerts and incidents as the old APs go down; this must be coordinated with the NOC (Network Operations Center) by either providing a list of APs participating each night in the upgrade or by suppressing the alerts until the new ones are up. The second fact to consider is the asset management update; new APs must be added to the system, including setting static IP addresses, if necessary, in Infoblox or the IPAM software/server in use. After repeating this cycle as many times as needed, it's 100% guaranteed the network upgrade will be a success. This phase is more time-consuming and physically demanding than proof of concept; it will require extensive overnights and months of hard work depending on the current AP location, access to the facilities and cable infrastructure in place.

Validation – Optimization

At this point in the process, we have all the core equipment (routers, switches, and controllers) fully operational and the new access points. It is time to finally test the network to see if 802.11ax is working as expected. To start with, it is highly recommended to conduct a passive site survey so we can confirm SNR and RSSI are reaching the desired values established during the predictive study; usually, according to Cisco and general guidelines, a RSSI = -67 dbm is the goal. Also, the appropriate maps must be uploaded to the application and all the materials that could affect the signal, like drywall, metal structures, and glass, must be considered. Testing in each location with all on-site employees is ideal, as the human body also absorbs a good portion of the signals; plus, it is recommended that the engineer running the survey can access all areas inside the building and populate the map 100%.

Once the survey is completed by location, the last step will be to evaluate the results and optimize the network if necessary. This involves usually adjusting the power level on the APs so the users can have better coverage, possibly by modifying the RF profile on the AP in question; these changes will depend on the needs of that area where the issue was found and the final goal to achieve, for instance, if there is an issue in a conference room as it's too big, we might need to deploy a 2nd AP. This feedback must be taken to the design/architecture team to propose a long-term solution that will satisfy the needs of the end users. The Ekahau heat map example below uses the sidekick sensor to capture the data as part of the equipment needed for site surveys.

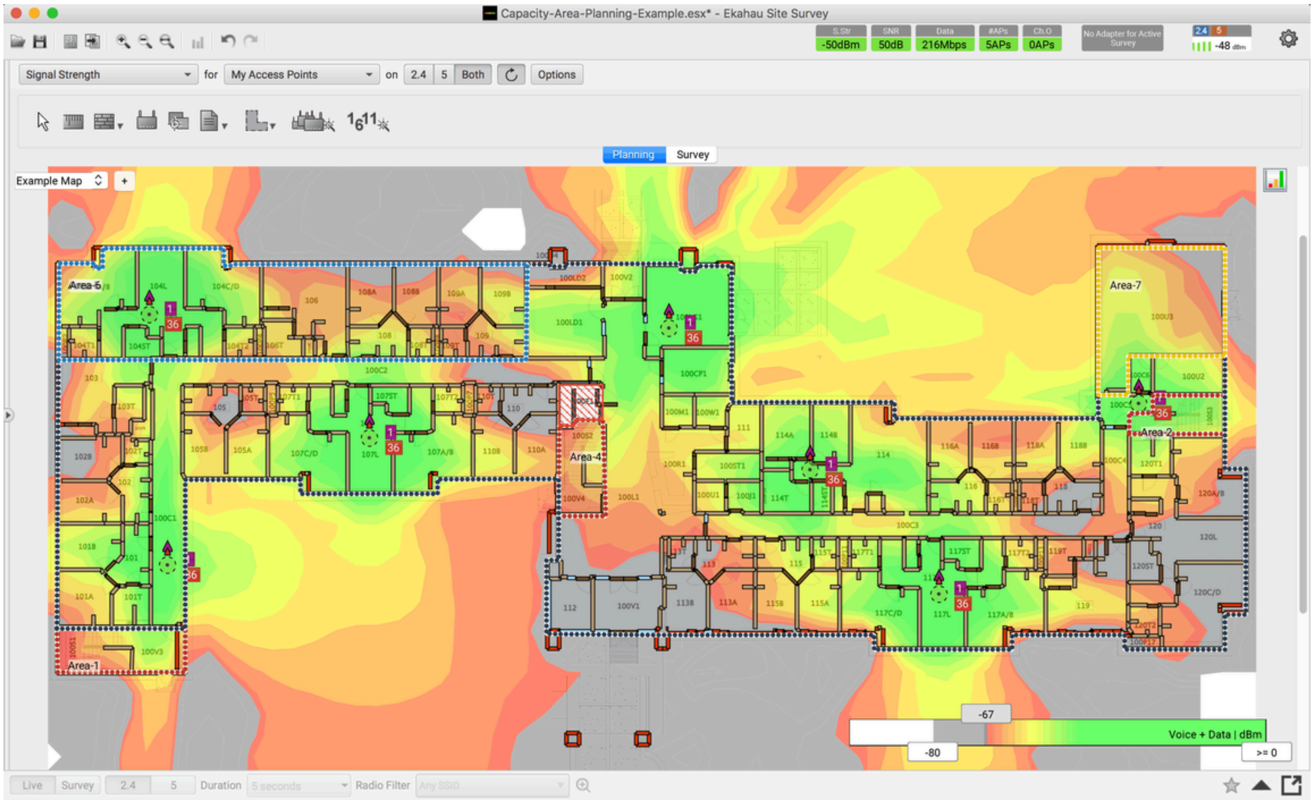

Figure 6. Ekahau heat map

Figure 6. Ekahau heat map

Conclusion

Upgrading a wireless network is a process that requires a specific skillset; besides the wireless knowledge and capabilities we as wireless engineers have, there are multiple components like offering leadership and guidance to others on how to move forward with this type of project, always keeping in mind that the final user is never affected. After making an upgrade of this magnitude, it is evident that 802.11ax can offer many advantages in comparison to 802.11n or 802.11ac, as it was designed with High Efficiency in mind, the daily tasks we all need to accomplish at work will be done quicker, as the technology uses better modulation techniques like 1024-QAM and OFDMA. Wireless networks will keep evolving daily, as it is how technology works and adapts itself to satisfy the high demand of a world that relies increasingly on devices that allow us to communicate globally and accomplish our assignments no matter where we are.